ABSTRACT

The present invention pertains to the fields of electrical communications and computer techniques and more precisely relates to cryptographic methods and devices for the ciphering of digital data. This method comprises splitting a data block into $N \geq 2$ sub-blocks and sequentially converting said sub-blocks by applying at least one conversion operation on the i-th sub-block, where $i \leq N$, said operation depending on the value of the j-th sub-block where $j \leq N$. This method is characterized in that the operation depending on the value of the j-th sub-block is a transposition operation of the bits in the i-th sub-block. This method is also characterised in that the transposition operation of the bits in the i-th sub-block, which depends on the value of the j-th cub-block, is carried out according to a secret key before the beginning of the i-th sub-block conversion. This method is further characterised in that a binary vector V is determined prior to the current transposition operation of the bits in the i-th sub-block, which depends on the j-th sub-block, wherein said transposition operation of the bits in the i-th sub-block is carried out according to the value of the vector V. The binary vector is determined according to its value when carrying out the preceding conversion step of one of the sub-blocks and according to the value of the j-th sub-block.